Appl. No. 10/081,061
Amdt. sent October 12, 2006
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group 2134

PATENT

REMARKS/ARGUMENTS

Claims 20-35 are pending in the application. Claim 20 has been amended. Support for the claims can be found in the specification as originally filed. No new matter has been introduced by virtue of these amendments.

Claims 20-35 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Claim 20 has been amended to recite in part "at least one cipher key commonly used among a plurality of security levels for each file." Support for "at least one cipher key" can be found at page 32, lines 7-23 of the present specification as originally filed. The Section 112 rejection of the claims is believed to be overcome.

Claims 20-23, 25-26, 28-29, and 33-35 were rejected under 35 U.S.C. §103(a) as being unpatentable over Boebert et al. (U.S. Patent No. 4,713,753) in view of McCollum et al. (U.S. Patent No. 6,006,228) and Matyas Jr. et al. (U.S. Patent No. 6,947,556). These claim rejections are overcome as follows.

Claims 24 and 27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Boebert et al. in view of McCollum et al. and Matyas Jr. et al. and further in view of Digital Equipment Corporation.

Claim 30 was rejected under 35 U.S.C. §103(a) as being unpatentable over Boebert et al. in view of McCollum et al. and Matyas Jr. et al. and further in view of Scheidt et al. (U.S. Patent No. 6,754,820).

Claims 31-32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Boebert et al. in view of McCollum et al. and Matyas Jr. et al. and further in view of Dryer et al. (U.S. Patent Publication No. 2002/0099666).

Interview with Examiner

A telephonic interview with the Examiner was conducted on October 10, 2006. The undersigned would like to thank the Examiner for his time. As understood, the Examiner

PATENT

indicated that Applicant's proposed claim amendments appear to overcome the current cited references.

Section 103 Rejections

Independent claim 20 has been amended to more clearly recite in part "an access control processing unit ... wherein if a host OS program of the access control processing unit is tampered, a guest OS of the access control processing unit is instructed to invalidate the functions of the host OS program." Support for this feature can be found, e.g., at page 29, lines 5-28 and FIG. 1 of the present specification as originally filed.

The Boebert reference discloses a "method of restricting access on the basis of predetermined relations between data format and subsystems [that] can be used to maintain the incorruptability of information." See, e.g., column 7, lines 33-37. A memory address apparatus compares an access right against operation and verifies that the modes and manners of access and manipulation required by the operation are permitted by the access right (see, e.g., column 9, lines 21-26).

The McCollum reference discloses a file table 200 which is used to control access to individual HTML documents. See, e.g., column 3, lines 5-6. The McCollum reference also discloses determining whether a user has the required security level and user group to access a desired file (see, e.g., column 3, lines 55-57).

The Matyas reference discloses secure access to an encrypted file utilizing two-level encryption where a file is encrypted with a first key and where that key is encrypted with a second key generated from a password associated with the encrypted file (see, e.g., column 8, lines 25-30).

The cited references simply teach allowing users to securely access desired files. While the cited references disclose secure access to encrypted files, the cited references do not teach or suggest protecting against illegal action against a host OS program of an access control processing unit. The claimed invention teaches this distinguishing feature of protecting against illegal action (tampering) against a host OS program used to confirm secure access to desired files. If the host OS program is tampered, the guest OS is instructed to invalidate the functions

Page 6 of 7

RECEIVED
CENTRAL FAX CENTER

OCT 1 2 2006

of the host OS, for example, by inhibiting all file accesses or stopping the execution of the host OS. See, e.g., page 29, lines 5-28 of the present specification as originally filed.

Even if combined, the combination of the cited references fails to teach or suggest "an access control processing unit ... wherein if a host OS program of the access control processing unit is tampered, a guest OS of the access control processing unit is instructed to invalidate the functions of the host OS program" as recited in independent claim 20.

Based upon the failure of the references relied upon the Examiner to teach or suggest the elements of independent claim 20, it is respectfully asserted that claim 20 and claims 21-35 depending therefrom, are patentable. The Section 103 rejection of the claims is believed to be overcome.
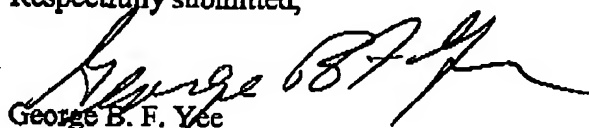
For at least the foregoing reasons, it is respectfully asserted that claims 21-35 depending from claim 20 are likewise are patentable over the art of record. The Section 103 rejections of the claims are believed to be overcome.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

George B. F. Yee
Reg. No. 37,478

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
GBFY:cl
60870441 v1